Proc. Indian Acad. Sci. (Math. Sci.) Vol. 114, No. 1, February 2003, pp. 1–6.
Printed in India

On some congruence with application to exponential sums

SOON-MO JUNG

Mathematics Section, College of Science and Technology, Hong-Ik University,
339-701 Chochiwon, Korea
E-mail: smjung@wow.hongik.ac.kr

MS received 19 July 2003; revised 17 November 2003

Abstract. We will study the solution of a congruence, $x \equiv g^{(1/2)\omega_g(2^n)} \bmod 2^n$, depending on the integers g and n, where $\omega_g(2^n)$ denotes the order of g modulo 2^n. Moreover, we introduce an application of the above result to the study of an estimation of exponential sums.

Keywords. Congruence; multiplicative order; exponential sum.

1. Introduction

Divisibility is an essential property between elements of algebraic structures. As we know, the concept of congruence originates from that of divisibility and it is not only a convenient notation but also a very helpful method to prove many theorems in number theory. For this reason, almost every textbook for number theory treats this topic extensively (cf. [2,3]).

There are very close relationships between the congruences and the exponential sums. In general, we may frequently use the properties of congruences to estimate any exponential sum (see [1,4,6]).

Discrepancy is also an important concept (or quantity) of number theory. It measures the deviation of the sequence from an ideal distribution and can be applied to problems in numerical analysis. We can easily calculate, e.g., by the inequality of Erdös–Turán, the upper bound of the discrepancy if the related exponential sum has been estimated. So, the estimations of the exponential sums are very interesting.

Let g and $m > 0$ be relatively prime integers. The (multiplicative) *order* of g modulo m is defined as the least positive exponent k such that $g^k \equiv 1 \bmod m$, and we will denote it by $\omega_g(m)$, i.e.,

$$\omega_g(m) \;=\; \min\{k \in \mathbb{N} : g^k \equiv 1 \bmod m\}.$$

In this paper, we investigate the solutions of a congruence related to the order of an odd integer modulo 2^n. These results will be applied to the study of an estimation of exponential sums.

2. Congruence modulo 2^n

For a positive integer n and an odd integer g, we recall that the order of g modulo 2^n is defined by

$$\omega_g(2^n) \;=\; \min\{k \in \mathbb{N} : g^k \equiv 1 \bmod 2^n\}.$$

Lemma 1. *Given an $n \in \mathbb{N}$, assume that g is an odd integer such that $g \not\equiv \pm 1 \bmod 2^n$. Then*

$$\omega_g(2^{n+1}) \;=\; 2\omega_g(2^n).$$

Proof. By the definition, we have $g^{\omega_g(2^n)} \equiv 1 \bmod 2^n$, i.e., $g^{\omega_g(2^n)} = a2^n + 1$ for some $a \in \mathbb{Z}$. Thus, for $k = 1, \ldots, \omega_g(2^n) - 1$, we obtain

$$g^k g^{\omega_g(2^n)} \;=\; ag^k 2^n + g^k \;\not\equiv\; 1 \bmod 2^{n+1},$$

since g^k is odd and $g^k \not\equiv 1 \bmod 2^n$. (If $ag^k 2^n + g^k \equiv 1 \bmod 2^{n+1}$, then there is an integer b with $ag^k 2^n + g^k = b2^{n+1} + 1$ and hence $(ag^k - 2b)2^n + g^k = 1$, i.e., $g^k \equiv 1 \bmod 2^n$, a contradiction.)

However, it holds that

$$\begin{aligned} g^{\omega_g(2^n)} g^{\omega_g(2^n)} &= ag^{\omega_g(2^n)} 2^n + g^{\omega_g(2^n)} \\ &= a(a2^n + 1)2^n + a2^n + 1 \\ &= a^2 2^{2n} + a2^{n+1} + 1 \\ &\equiv 1 \bmod 2^{n+1}. \end{aligned}$$

Therefore, it holds that $\omega_g(2^{n+1}) = 2\omega_g(2^n)$. □

Remark 1. If $n \geq 2$ is an integer and g is an odd integer with $g \not\equiv \pm 1 \bmod 2^n$, then the previous lemma implies that $\omega_g(2^n) = 2\omega_g(2^{n-1})$. If $g \equiv -1 \bmod 2^n$ then $\omega_g(2^n) = 2$. Thus, for $n \geq 2$ and $g \not\equiv 1 \bmod 2^n$, $(1/2)\omega_g(2^n)$ is a positive integer.

The following lemma reveals that the congruence $x \equiv g^{(1/2)\omega_g(2^n)} \bmod 2^n$ has at most three distinct solutions (modulo 2^n). However, as we see in Lemmas 3 and 4 below, the congruence can have only two distinct solutions, -1 and $2^{n-1} + 1$ modulo 2^n, indeed.

Lemma 2. *Assume that n is an integer ≥ 3 and g is an odd integer with $g \not\equiv 1 \bmod 2^n$. Every solution of the following congruence*

$$x \;\equiv\; g^{(1/2)\omega_g(2^n)} \bmod 2^n$$

is congruent to one of $\{-1, 2^{n-1} - 1, 2^{n-1} + 1\}$ modulo 2^n.

Proof. Since g is odd, so is $g^{(1/2)\omega_g(2^n)}$. Set

$$g^{(1/2)\omega_g(2^n)} \;=\; a2^{n-1} + 2k + 1, \tag{1}$$

where a and k are some integers with $0 \leq k < 2^{n-2}$. It then follows from the definition of $\omega_g(2^n)$ that

$$\begin{aligned} g^{\omega_g(2^n)} &= (a2^{n-1} + 2k + 1)^2 \\ &= 2^n(a^2 2^{n-2} + a(2k+1)) + 4k^2 + 4k + 1 \\ &\equiv 1 \bmod 2^n. \end{aligned}$$

Therefore, we get $2^n | (4k^2 + 4k)$, i.e., $2^{n-2} | k(k+1)$.

(a) Suppose k is odd. Then, $k+1$ is even. Hence, it follows that $2^{n-2}|(k+1)$. As $1 \leq k+1 \leq 2^{n-2}$, we conclude that $k+1 = 2^{n-2}$. Due to (1), we have

$$g^{(1/2)\omega_g(2^n)} + 1 \;=\; (a+1)2^{n-1}.$$

If we square both sides of the last equality, then

$$g^{\omega_g(2^n)} + 2g^{(1/2)\omega_g(2^n)} + 1 \;=\; (a+1)^2 2^{2n-2}.$$

As $g^{\omega_g(2^n)} \equiv 1 \bmod 2^n$, it follows from the last equality that $2 + 2g^{(1/2)\omega_g(2^n)} \equiv 0 \bmod 2^n$, i.e., $1 + g^{(1/2)\omega_g(2^n)} \equiv 0 \bmod 2^{n-1}$. By (1) and the last congruence, we have $k+1 \equiv 0 \bmod 2^{n-2}$, i.e., there exists an integer b such that $k = b2^{n-2} - 1$. If $a+b$ is even, it then follows from (1) that $g^{(1/2)\omega_g(2^n)} \equiv -1 \bmod 2^n$. If $a+b$ is odd, we get $g^{(1/2)\omega_g(2^n)} \equiv 2^{n-1} - 1 \bmod 2^n$.

(b) Now, suppose k is even. Then, it holds that $2^{n-2}|k$. As $0 \leq k < 2^{n-2}$, it must be $k = 0$. Due to (1), we obtain

$$g^{(1/2)\omega_g(2^n)} \;=\; a2^{n-1} + 1.$$

If a is even, then $g^{(1/2)\omega_g(2^n)} \equiv 1 \bmod 2^n$ and $(1/2)\omega_g(2^n) < \omega_g(2^n)$, a contradiction. Hence, a is odd and $g^{(1/2)\omega_g(2^n)} \equiv 2^{n-1} + 1 \bmod 2^n$. □

In the previous lemma, we have proved that if $n \geq 3$ and g ($\not\equiv 1 \bmod 2^n$) is an odd integer, it may occur that $g^{(1/2)\omega_g(2^n)} \equiv -1 \bmod 2^n$. In the following lemma, we will prove that if $g \not\equiv -1 \bmod 2^n$ then $g^{(1/2)\omega_g(2^n)} \not\equiv -1 \bmod 2^n$.

Lemma 3. *Assume that n is an integer* ≥ 3 *and g is an odd integer with* $g \not\equiv 1 \bmod 2^n$. *If the congruence*

$$g^{(1/2)\omega_g(2^n)} \;\equiv\; -1 \bmod 2^n$$

holds, then $\omega_g(2^n) = 2$ *and* $g \equiv -1 \bmod 2^n$.

Proof. Set $g = 2k+1$ with some $k \in \mathbb{Z}\backslash\{0\}$. By the binomial theorem, we have

$$\begin{aligned} g^{(1/2)\omega_g(2^n)} &= (2k+1)^{(1/2)\omega_g(2^n)} \\ &= \sum_{i=0}^{(1/2)\omega_g(2^n)} \binom{(1/2)\omega_g(2^n)}{i} (2k)^i. \end{aligned} \tag{2}$$

Assume that $g \not\equiv -1 \bmod 2^n$. It follows from Lemma 1 that $\omega_g(2^n) = 2^2\omega_g(2^{n-2})$. Hence,

$$\frac{1}{2}\omega_g(2^n) \;=\; \binom{(1/2)\omega_g(2^n)}{1}$$

is even. Therefore, it follows from (2) and the given congruence that

$$\begin{aligned} g^{(1/2)\omega_g(2^n)} &= 1 + \sum_{i=1}^{(1/2)\omega_g(2^n)} \binom{(1/2)\omega_g(2^n)}{i} (2k)^i \\ &= 1 + 2^2 m \\ &\equiv -1 \bmod 2^n, \end{aligned}$$

where m is an appropriate integer. Hence, $2^2 m \equiv -2 \bmod 2^n$ or $2^2 m = a2^n - 2$ for some $a \in \mathbb{Z}$. Thus, we have $m = a2^{n-2} - 1/2$, which is a contradiction. Hence, it follows that $g \equiv -1 \bmod 2^n$. Moreover, we see that $\omega_g(2^n) = 2$. $\square$

In view of Lemma 2, we may expect that the congruence $g^{(1/2)\omega_g(2^n)} \equiv 2^{n-1} - 1 \bmod 2^n$ holds for some $n \geq 3$ and some odd integer g. However, we have to give up our expectation as we see in the following lemma.

Lemma 4. *Assume that n is an integer ≥ 3 and g is an odd integer with $g \not\equiv 1 \bmod 2^n$. The congruence*

$$g^{(1/2)\omega_g(2^n)} \equiv 2^{n-1} - 1 \bmod 2^n$$

does not hold.

Proof. If we set $g = 2k+1$ with some $k \in \mathbb{Z} \backslash \{0\}$ and follow the first part of the proof of Lemma 3, we then obtain (2).

(a) Assume that $g \not\equiv -1 \bmod 2^n$. By following the second part of the proof of Lemma 3, we have

$$g^{(1/2)\omega_g(2^n)} = 1 + 2^2 m \equiv 2^{n-1} - 1 \bmod 2^n,$$

where m is some integer. Thus, $2^2 m \equiv 2^{n-1} - 2 \bmod 2^n$ or $2^2 m = a2^n + 2^{n-1} - 2$ for some $a \in \mathbb{Z}$. Hence, we get $m = a2^{n-2} + 2^{n-3} - 1/2$, which is a contradiction.

(b) If $g \equiv -1 \bmod 2^n$, then $\omega_g(2^n) = 2$. Therefore, the given congruence reduces to $g \equiv 2^{n-1} - 1 \bmod 2^n$. Altogether, it follows that $2^{n-1} - 1 \equiv -1 \bmod 2^n$, which is a contradiction. $\square$

In the following theorem, we will summarize all the results of lemmas 2, 3 and 4.

Theorem 5. *Let n be a given integer larger than 2 and let g be a given odd integer.*

(a) *If $g \not\equiv \pm 1 \bmod 2^n$, then*

$$g^{(1/2)\omega_g(2^n)} \equiv 2^{n-1} + 1 \bmod 2^n.$$

(b) *If $g \equiv -1 \bmod 2^n$, then*

$$g^{(1/2)\omega_g(2^n)} \equiv -1 \bmod 2^n.$$

3. Application to exponential sums

For any non-zero integer w, we denote by $d(w)$ the *greatest exponent k* of 2 satisfying $2^k | w$, i.e., $d(w) = \max\{k \in \mathbb{N}_0 : 2^k | w\}$, and we use the notation $2^{d(w)} \| w$ for this case.

Remark 2. Every non-zero integer w can be represented by $w = 2^{d(w)} w_0$, where w_0 is an odd integer.

For an odd integer $g \notin \{-1,1\}$, we define

$$c(g) \;=\; \begin{cases} \min\{k \in \mathbb{N} : g < 2^{k-1}-1\} & \text{for } g > 1, \\ \min\{k \in \mathbb{N} : g > -2^{k-1}-1\} & \text{for } g < -1. \end{cases}$$

In this section, we will introduce an application of the previous results. Indeed, Korobov [5] has already proved a similar result in the following theorem. However, our proof is more visible than that of Korobov.

Theorem 6. *If $g \notin \{-1,1\}$ is an odd integer and w is a non-zero integer, then*

$$\sum_{k=1}^{\omega_g(2^n)} e^{2\pi i w g^k/2^n} = 0$$

for any integer $n \geq d(w) + \max\{3, c(g)\}$.

Proof.

(a) Assume that w is odd. As $n \geq c(g)$, if $g > 1$ then $1 < g < 2^{n-1}-1$. Similarly, if $g < -1$ then $2^{n-1}-1 < 2^n + g < 2^n - 1$. Hence, we conclude that $g \not\equiv \pm 1 \bmod 2^n$.
It follows from Theorem 5(a) that

$$g^{(1/2)\omega_g(2^n)} \;\equiv\; 2^{n-1}+1 \bmod 2^n$$

or

$$g^{(1/2)\omega_g(2^n)} \;=\; a2^n + 2^{n-1} + 1 \tag{3}$$

for some $a \in \mathbb{Z}$.
Since g^k is odd, (3) yields

$$\begin{aligned} g^{k+(1/2)\omega_g(2^n)} &= ag^k 2^n + g^k 2^{n-1} + g^k \\ &\equiv 2^{n-1} + g^k \bmod 2^n \end{aligned}$$

for $k = 1, \ldots, (1/2)\omega_g(2^n)$. Moreover, since w is assumed to be odd, we get

$$\begin{aligned} wg^{k+(1/2)\omega_g(2^n)} &\equiv w2^{n-1} + wg^k \bmod 2^n \\ &\equiv 2^{n-1} + wg^k \bmod 2^n. \end{aligned} \tag{4}$$

Hence, it follows from (4) that

$$\begin{aligned} \sum_{k=1}^{\omega_g(2^n)} e^{2\pi i w g^k/2^n} &= \sum_{k=1}^{(1/2)\omega_g(2^n)} \left(e^{2\pi i w g^k/2^n} + e^{2\pi i w g^{k+(1/2)\omega_g(2^n)}/2^n}\right) \\ &= \sum_{k=1}^{(1/2)\omega_g(2^n)} \left(e^{2\pi i w g^k/2^n} + e^{2\pi i (2^{n-1}+wg^k)/2^n}\right) \\ &= 0. \end{aligned}$$

(b) Assume now that w is a non-zero even integer. As we noticed in Remark 2, w may be represented as $w = 2^{d(w)} w_0$, where w_0 is odd. If we set $m = n - d(w)$, we obtain $g \not\equiv \pm 1 \bmod 2^m$ by following the first part of (a).
It follows from Theorem 5(a) that

$$g^{(1/2)\omega_g(2^m)} \equiv 2^{m-1} + 1 \bmod 2^m.$$

By a similar method given in (a), we get, instead of (4),

$$w_0 g^{k+(1/2)\omega_g(2^m)} \equiv 2^{m-1} + w_0 g^k \bmod 2^m$$

for $k = 1, \ldots, (1/2)\omega_g(2^m)$. As we did in the last part of (a), we have

$$\sum_{k=1}^{\omega_g(2^m)} \mathrm{e}^{2\pi i w_0 g^k / 2^m} = 0. \tag{5}$$

According to Lemma 1, we get

$$\omega_g(2^n) = 2^{d(w)} \omega_g(2^m). \tag{6}$$

Finally, it follows from (5) and (6) that

$$\begin{aligned} \sum_{k=1}^{\omega_g(2^n)} \mathrm{e}^{2\pi i w g^k / 2^n} &= \sum_{k=1}^{\omega_g(2^n)} \mathrm{e}^{2\pi i w_0 g^k / 2^m} \\ &= 2^{d(w)} \sum_{k=1}^{\omega_g(2^m)} \mathrm{e}^{2\pi i w_0 g^k / 2^m} \\ &= 0, \end{aligned}$$

as required. □

Acknowledgement

This work was supported by the 2004 Hong-Ik University Academic Research Support Fund.

References

[1] Brown G, Moran W and Pearce C E M, Riesz products and normal numbers, *J. London Math. Soc.* (2) **32** (1985) 12–18
[2] Cassels J W S, On a problem of Steinhaus about normal numbers, *Coll. Math.* **7** (1959) 95–101
[3] Colebrook C M and Kemperman J H B, On non-normal numbers, *Indag. Math.* **30** (1968) 1–11
[4] Drmota M and Tichy R F, Sequences, discrepancies and applications (Berlin/Heidelberg: Springer) (1997)
[5] Korobov N M, Trigonometric sums with exponential functions and the distribution of signs in repeating decimals, *Math. Notes* **8** (1970) 831–837
[6] Kuipers L and Niederreiter H, Uniform distribution of sequences (J. Wiley and Sons) (1974)